UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/648,555	08/25/2003	Stuart Cain	200310064-1	5177

22879 7590 07/17/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
WYSZYNSKI, AUBREY H	
ART UNIT	**PAPER NUMBER**
2134	

MAIL DATE	DELIVERY MODE
07/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/648,555	CAIN, STUART	
	Examiner	Art Unit	
	Aubrey H. Wyszynski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *8/25/03* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 4/16/07 was received and considered

2. Claims 1-20 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 1-9 have been considered but are moot in view of the new ground(s) of rejection.

4. Applicant's arguments with respect to claims 10-20 have been fully considered but they are not persuasive. Applicant argues Schneier does not teach components included in a highest risk path or attacking spreading between these components. The examiner respectfully disagrees. Schneier teaches identifying a highest risk path in the several examples of sample attack trees described in the specification. Additionally, Schneier illustrates an attack tree flow chart and an overall security evaluation in Figure 5. Please see the rejection below for further clarification.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, U.S. Patent No. 5,850,516 and further in view of Burrows et al, U.S. Patent Application Publication No. 2002/0073338.

Regarding claim 1, Schneier discloses a security intrusion mitigation method comprising: utilizing network spanning tree configuration information to determine an action for mitigating diffusion of intrusive attacks between components associated with a the network, wherein said spanning tree information includes an indication of an internal diffusion risk, wherein said internal diffusion risk is a risk of said attack diffusing from a first component associated with said network to a second component associated with said network; and performing said action for mitigating diffusion of intrusive attacks automatically, wherein said action for mitigating includes compensation for functional support of prioritized applications (col. 3, lines 10-27). Schneier lacks or does not expressly disclose wherein said internal diffusion risk is a risk of said attack diffusing from a first component associated with said network to a second component associated with said network; and performing said action for mitigating diffusion of intrusive attacks automatically, wherein said action for mitigating includes compensation for functional support of prioritized applications. However, Burrows discloses wherein said internal diffusion risk is a risk of said attack diffusing from a first component associated with said network to a second component associated with said network (¶[0040-0041]); and performing said action for mitigating diffusion of intrusive attacks automatically (¶[0028]); wherein said action for mitigating includes compensation for functional

support of prioritized applications (¶[0036]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schneier with the method of Burrows to diffuse attack from a first component to a second component in the network in order to mitigate the effects of undesirable behavior on the network, as taught by Burrows (¶[0028]).

Regarding claim 2, Schneier as modified above further discloses a security intrusion mitigation method of claim 1 further comprising utilizing said internal diffusion risk values to determine components forming a path in said spanning tree configuration with a highest cumulative diffusion impact risk (fig. 5).

Regarding claim 3, Schneier as modified above further discloses a security intrusion mitigation method of claim 1 wherein said internal diffusion risk includes an asset value factor/leaf node values (fig. 5, #540).

Regarding claim 4, Schneier as modified above further discloses a security intrusion mitigation method of claim 3 wherein said asset value corresponds to an economic impact of a disruption to functionality provided by a network component (col. 8, lines 46-65).

Regarding claim 5, Schneier as modified above further discloses a security intrusion mitigation method of claim 1 wherein said internal diffusion risk includes an exposure

rating factor (col. 9, lines 24-27).

Regarding claim 6, Schneier discloses a security intrusion mitigation method of claim 5 wherein said exposure rating defines a threshold value corresponding to connectivity of a network component with other network components (col. 17, lines 62-67).

Regarding claim 7, Schneier as modified above further discloses a security intrusion mitigation method of claim 5 wherein said network component is assigned an exposure rating value based upon a connectivity distance from a root node (fig. 6).

Regarding claim 8, Schneier as modified above further discloses a security intrusion mitigation method of claim 5 wherein said action for mitigating diffusion of intrusive attacks is implemented in accordance with a highest risk algorithm (col. 22, lines 38-52).

Regarding claim 9, Schneier as modified above further discloses a security intrusion mitigation method of claim 5 wherein said network spanning tree configuration information includes information associated with components included in a utility data center and said mitigation action is implemented in said utility data center (col. 5, lines 1-25).

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 10, 13-17 and 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Schneier, U.S. Patent No. 5,850,516.

Regarding claim 10, Schneier discloses a security intrusion mitigation system comprising: a means for communicating information (fig. 1); a means for processing information including instructions for determining a highest risk path and automatically mitigating an attack from spreading between components included in said highest risk path (fig. 5, col. 3, lines 15-16 and col. 15 line 37-col. 16, line 12); and a means for storing said information, including instructions for storing information describing said highest risk path (fig. 2, #260).

Regarding claim 13, Schneier discloses a security intrusion mitigation system of claim 10 wherein said instructions include attack spread risk determination instructions (fig. 5).

Regarding claim 14, Schneier discloses a security intrusion mitigation system of claim 10 further comprising a means for centrally controlling utility data center operations (col. 5, lines 1-25).

Regarding claim 15, Schneier discloses a computer usable storage medium having computer readable program code embodied therein for causing a computer system to implement security intrusion mitigation instructions comprising: a component risk determination module for determining a risk of an attack spreading from a first component to a second component included in a network (col. 4, lines 5-6 and lines 19-21); and an attack spreading response module for responding to said risk of said attack spreading from said first component to said second component included in said network (col. 15, lines 38-66).

Regarding claim 16, Schneier discloses a computer usable storage medium of claim 15 wherein said risk is biased based upon an economic value of functions said second component performs (col. 8, lines 46-65).

Regarding claim 17, Schneier discloses a computer usable storage medium of claim 15 said risk is biased based upon connectivity of said second component to said first component in said network (fig. 6).

Regarding claim 20, Schneier discloses a computer readable medium of claim 19 wherein said response is performed in accordance with an highest risk analysis (fig. 5).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 11-12 and 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier as applied to claims 10, 15 and 17 above, and further in view of Fox et al, U.S. Patent No. 6,535,227.

Regarding claim 11, Schneier discloses a security intrusion mitigation system of claim 10. Schneier lacks or does not expressly disclose wherein said instructions include security management instructions implemented on a network application management platform. However, Fox discloses wherein said instructions include security management instructions implemented on a network application management platform (col. 3, lines 46-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Schneier with the device of Fox to include a network application management platform in order to edit properties of the network nodes for network design alternatives, as taught by Fox (col. 3, lines 60-63).

Regarding claim 12, Schneier discloses a security intrusion mitigation system of claim 10. Schneier lacks or does not expressly disclose a means for interfacing with a network application management platform. However, Fox discloses a means for

interfacing with a network application management platform (col. 3, lines 46-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Schneier with the device of Fox to include a network application management platform in order to edit properties of the network nodes for network design alternatives, as taught by Fox (col. 3, lines 60-63).

Regarding claim 18, Schneier discloses a computer usable storage medium of claim 17. Schneier lacks or does not expressly disclose wherein said response includes reducing traffic communication to said second component. However, Fox wherein said response includes reducing traffic communication to said second component (col. 12, lines 16-30). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Schneier with the device of Fox to reduce traffic communication in order to reduce one or more vulnerabilities, as taught by Fox, (col. 12, lines 16-30).

Regarding claim 19, Schneier discloses a computer usable storage medium of claim 15. Schneier lacks or does not expressly disclose wherein said response includes turning off an interface of said second component to said network. However, Fox discloses wherein said response includes turning off an interface of said second component to said network (col. 12, lines 16-30). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Schneier with the device of Fox to turn off an interface in order to reduce one or more vulnerabilities, as

taught by Fox, (col. 12, lines 16-30).

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Wyszynski whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, and alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 5712723811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AHW

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER